RELATION OF THE THEORY OF CERTAIN TRINOMIAL EQUATIONS IN A FINITE FIELD TO FERMAT'S LAST THEOREM

By H. S. Vandiver

UNIVERSITY OF TEXAS

Communicated August 22, 1955

1. In several previous papers1, 2, 3, 4 the writer brought out a relation between a certain theory of trinomial congruences and the second case of Fermat's Last Theorem. In this work the aim was to employ powerful tools from each of two deep theories in number theory and to unify the methods employed. Of course, it would be nice to prove the Fermat theorem, and by any means possible; but failing this, any by-products derived from such a failure are more likely to be novel and of value if we employ initially what appear to be some of the important results in algebraic number theory than if we stay with elementary results and method.

The depth of the first theory mentioned above is well known; it includes the theory of the laws of reciprocity, class numbers, and class fields in the theory of algebraic fields, and stemmed originally from the consideration of the conditional binomial congruence

\[ x^n \equiv \theta \pmod{p}, \]

where \( p \) is a prime ideal in an algebraic field \( K \) and \( \theta \) an integer in \( K \), not an \( n \)th power in \( K \). This led to laws of reciprocity for special values of \( n \) (generalizing quadratic reciprocity) and particularly for \( l \)th powers, where \( l \) is a regular prime,
and the other topics mentioned above followed in its wake. However, the depth of the second topic is not so well known, and I should like to explain my viewpoint here. The latter theory had its beginnings in the work of Lagrange in his contributions to cyclotomy, mainly his use of the Lagrange resolvent. Then Gauss's work in exponential sums (cyclotomic periods) led, for special values of \( m \), to the consideration of the congruence

\[ ax^m + by^m \equiv d \pmod{p}, \]

where all the symbols represent rational integers. Then, based on the Lagrange resolvent

\[ \tau(a, \xi) = a + \xi a^r + \xi^2 a^{r^2} + \ldots + \xi^{r-2} a^{r^{r-2}}, \]  

(A)

where \( \xi = e^{2\pi i/l}, \alpha = e^{2\pi i/p}, p = 1 + lm, r \) is a primitive root of \( p \), and \( l \) is an odd prime. Cauchy, Jacobi, and Eisenstein studied the sum

\[ \psi(\alpha) = \sum_h \alpha^{-bh + (a + b) \text{ ind } (\xi^h + 1)}, \]  

(B)

where \( h \) ranges over all the integers \( 0, 1, \ldots, p - 2 \), excepting \( (p - 1)/2 \), and

\[ q^{\text{ind } x} \equiv x \pmod{p}. \]

These numbers (A) and (B) were further studied and extended by Kummer, Stickelberger, H. H. Mitchell, and, particularly since 1920, many others, and the literature is now vast. Many applications have been worked out, mainly to the theory of conditional equations in finite fields. And, in particular, we shall point out some work that has been done which perhaps illustrates best how far-reaching our topic is. Fueter used the complex multiplication of elliptic functions to generalize the Lagrange resolvent (A) and the Cauchy-Jacobi sum (B) and obtained exponential sums involving the use of a quadratic field and then the field obtained by adjoining a cyclotomic field to the former. This resulted in proofs of certain important known laws of reciprocity involving this extended field, so that here, in a sense, the two theories we mentioned at the beginning of our paper merge into one. It is this development and several others that led me to use the term "depth" in connection with our second general topic. The theory of the symbol \((i, j)_{c l}\) for \( c \) and \( l \) arbitrary (as defined just below our relation [7] for \( l \) prime), which is used so much in the present paper and in a number of our previous ones, has yielded applications to the theory of quadratic forms, the theories of congruences in algebraic fields, finite geometries, algebraic varieties in geometry, difference sets, and Diophantine analysis, as well as to the theory of cyclotomic fields.

2. Consider

\[ x^l + y^l + z^l = 0, \]  

(1)

\( l \) being an odd prime, \( xyz \not\equiv 0 \pmod{l} \), the so-called first case of equation (1). Let \( \xi = e^{2\pi i/l} \), and let \( \alpha \) be a primary integer in the field \( K(\xi) \) or \( K \) with \((\alpha, z(\xi - 1)) = 1\); then, from equation (1),

\[ (x + \xi^i y) = a_i^l, \]

(2)

\( i = 0, 1, \ldots, l - 1, a_i \) an ideal in \( K \). Then
\[
\left( \frac{\alpha}{x + t^iy} \right) = 1,
\]
i = 0, 1, \ldots, l - 1, and, since \( \alpha \) is primary, we have by the law of reciprocity for \( l \)th powers in \( K \),
\[
\left( \frac{x + \xi^iy}{\alpha} \right) = 1.
\tag{3}
\]
We now note also that if \( (\alpha) = b^h \), with \( b \) an ideal \( \epsilon K \) with \( (h, l) = 1 \), then equation (3) gives
\[
\left( \frac{x + \xi^iy}{b} \right) = 1.
\tag{3a}
\]
Note the difference in our discussion\(^2\) of the second case of the Fermat problem. Here we found that if \( y \equiv 0 \pmod{l} \),
\[
\left( \frac{x + \xi^iy}{b} \right) = 1,
\tag{4}
\]
where \( b \) is any ideal in \( K \) such that \( b^h \) is a principal ideal such that \( b^h = (\alpha) \), with \( \alpha \) in \( K \) and \( (h, l) = 1 \), whereas \( \alpha \) was limited to be primary, as we explained above for the first case of equation (1).

If, in equation (3a), we set \( b = p \), a prime ideal in \( K \), then it follows as elsewhere (relation (4) of an earlier paper\(^2\)), with \( \rho_i \in K \), that
\[
x + \xi^iy = \rho_i^l \pmod{p},
\tag{5}
i = 0, 1, \ldots, l - 1, \text{ and } p \text{ divides } (p) \text{ with } p \text{ an odd prime } > xyz.
\]
Consider the equation in the finite field \( F(p^n) \)
\[
g^{i+jx} + g^{i+j} = 1;
\tag{6}
p^n = 1 + cl = 1 + cpl^i, \text{ since } p^h \text{ is primary}; \text{ } i \text{ is in the set } 0, 1, \ldots, c - 1; \text{ } j \text{ is in the set } 0, 1, \ldots, l - 1; \text{ } s \text{ is in the set } 0, 1, \ldots, l - 1; \text{ } t \text{ is in the set } 0, 1, \ldots, c - 1; \text{ and } g \text{ is a multiplicative generator of the nonzero elements of } F(p^n). \text{ Now equation (5) may be written in the form (6), if we first write (5), using } s \text{ in place of } i, \text{ as}
\[
-\frac{y}{x} r^s + x^{i-1} \rho_i = 1 \pmod{p} \tag{7}
\]
and set \( \xi = g_1^c \pmod{p} \), \( -y/x = g_1^i, x^{-1} = g_1^i, \rho_i = g_1^i \); where \( g_1 \) is a primitive root of \( p \) in \( K \). The residue classes modulo \( p \) form a finite field of order \( p^n \), with \( p^n \) also the norm of \( p \) in \( K \). Hence \( g \) corresponds to \( g_1 \), and \( x \) and \( y \) have corresponding integral elements in the \( F(p^n) \). Hence relation (7) becomes relation (6) in \( F(p^n) \). In equation (6), represent the number of solutions \( s, t \) as \( (i, j)_{ct} \); then it follows from relation (7) that \( (i, j) = l \), an example\(^3\) of case \( A \) of equation (6).

3. Our work so far in examining equation (1) has made use of powerful tools in the first general theory mentioned in our introduction. We now apply some results which belong to the second topic mentioned at the beginning. In a previous
paper\(^2\) we obtained the relation, since \(p^n = 1 + cl^2\) and \(m\) is replaced by the odd prime \(l\),

\[
\sum_{i=0}^{l-1} (b, i)_{cl} (b - a, i - d)_{cl} = \sum_{j=0}^{c-1} (d, j)_{c(d - a, j - b)}_{c}, \tag{8}
\]

with \((i, j)_{c} = (i, j)_{cc}; d\) ranges over the set of distinct integers in the set 0, 1, \ldots, \(c - 1\) of the form \(d_1 + kl\), with \(d_1\) some integer and with \(0 < d_1 < l\).

If we take \(a = 0\) in equation (8) and \(d \neq 0 \pmod{l}\) and use \(b\) in place of \(i\) in \(g^i = y/x\), then we find\(^4\) that we have

\[
(d, i)_c(d, i - b)_c = 0, \tag{9}
\]

for any \(d \neq 0 \pmod{l}\), \(b \neq 0 \pmod{c}\), which we may use if we assume \(y/x \neq 1\) in \(F(p^n)\), which we may do when \(p\) is sufficiently large; \(i\) is any integer in the set 0, 1, \ldots, \(c - 1\). In another paper\(^4\) the writer gave the result that if \(p^n = 1 + cl\), with \((c, l) = 1, v = cl\),

\[
\sum_{i=0}^{m-1} (b, 1)_{cl} (b - a, j - d)_{cl} = \sum_{j=0}^{c-1} (d_1, j)_{c(d - a, j - b)}_{c}, \tag{10}
\]

where \(d\) ranges over \(d_1, d_1 + l, d_1 + 2l, \ldots, d_1 + (c - 1)l\), \(a\) and \(d_1\) are any integers such that we do not have both the relations \(d_1 \equiv 0 \pmod{l}\) and \(a \equiv 0 \pmod{c}\) holding. Now, if we examine the argument we gave to prove relation (10), we find that it will also hold if we assume that the only restriction on \(c\) and \(l\) is \(p^n = 1 + cl\). If we use it in this more general form, we may employ it to obtain relation (8). For, if we take relation (10) and substitute in turn \(d_1, d_1 + c, d_1 + 2c, \ldots, d_1 + (l - 1)c\), add the resulting equations, and employ the formula (relation (13) of an earlier paper\(^1\)),

\[
\sum_{r=0}^{m-1} (d_1 + rc, j - b)_{rc} = (d_1, j - b)_{c}, \tag{11}
\]

we have equation (8).

In a previous paper\(^2\) we found a relation of the type (7) applying to the second case of Fermat's Last Theorem, but as a relation in the finite field \(F(p)\), which corresponds to a congruence modulo \(p\), as then we had in mind the application of rapid computing machines to some of our related problems, and this was relevant since \(g\) in this case is a rational integer and \(p = 1 + cl\), that is, the special case when \(n = 1\).

Relation (1) shows that in relation (7) we may replace \(y/x\) by \(z/y, z/x, x/z, y/z, z/y\), and obtain relations similar to (6) involving equations in a finite field \(F(p^n)\), and in the same way we shall find that for these different pairs there exist an \(i\) and \(j\) in relation (6) such that \((b, h)_{cl} = l\) and \((b, l)_{cl} = 0\) for \(\neq h\) modulo \(l\). Hence we may employ equation (10) and find, as elsewhere (relation (11) of another paper\(^4\)),

\[
(d, i)_{c(d, i - b)}_{c} = 0 \tag{11}
\]

(where, if we replace \(l\) by \(v\) in eq. [6], then \((j, i)_{c}\) is the number of solutions \(t, s\) in eq. [6]), which we have already noted holds (in the present paper) for any \(c\) and \(m\) such that \(p^n = 1 + cm\), and we here set \(m = l\), an odd prime.)
If we use some previous results\(^1\) (p. 249) with relations (6) and (7) of the present paper, we may state

**Theorem I (first case).** Assume the following:
1. Relation (1) holds with \(xyz \equiv 0 \pmod{l}\), with \(l\) a given odd prime.
2. In the algebraic field defined by \(e^{2\pi i/l} \equiv \sqrt[l]{a}\) (say, \(K\)), let there be a prime ideal \(\mathfrak{p}\) such that \(\mathfrak{p}^h = (\theta)\), with \(h \not\equiv 0 \pmod{l}\) and \(\theta\) a primary integer in \(K\); also, \((p) \equiv 0 \pmod{p}\), where \(p\) is an odd rational prime >\(xyz\).

Then there exists a finite field \(F(p^n)\) of order \(p^n = 1 + cl\), \(c = cl\); and the norm of \(\mathfrak{p}\) is \(p^n\) for any \(p\) satisfying the last assumption and such that relations (9) hold, where \(d\) is any integer of the form \(d_1 + kl\), \(k = 0, 1, \ldots, c_1 - 1\), with \(d_1 \not\equiv 0 \pmod{l}\); \(i\) is any element of the set \(0, 1, \ldots, c - 1\); and if \(g\) is a multiplicative generator of the nonzero elements of \(F(p^n)\), then \(g^a\) takes on any one of the values

\[-y - x - z - x - y - z - x - z - y - \frac{z}{x} - \frac{y}{z} \text{ in } F(p^n)\]

The symbol \((h, k)\), for any \(h\) and \(k\), used in formula (9), is defined just below our relation (8).

**Theorem II (second case).** Assume the following:
1. Relation (1) holds with \(y \equiv 0 \pmod{l}\) \((xz, l) = 1\), \(y \not\equiv 0\), \(l\) a given odd prime.
2. Suppose that \(\mathfrak{p}\) is an ideal prime dividing \((p)\), where \(p\) is a rational odd prime >\(xyz\) in \(K(e^{2\pi i/l})\) and \(\mathfrak{p}^h\) is a principal ideal in \(K\) with \(h \not\equiv 0 \pmod{l}\), with \(p^n\) the norm of \(\mathfrak{p}\).

Then there exists a finite field of order \(p^n\) for every \(p\) satisfying the last assumption such that relations (11) hold in the finite field \(F(p^n)\), where \(g^h\) has either of the values

\[-y/x, -y/z, \text{ in } F(p^n)\]

---


\(^5\) (Œuvres, 2, 375, 1868.

\(^6\) It seems that the earliest published paper in which the number (B) appears is an article by Cauchy: Bull. sci. math. astr. phys. chim. (ed. Ferussac), 12, 205, 1829; Mem. Acad. Sci. Inst. France (Ser. 2), 17, 1840; In his Œuvres, Ser. 1, 3, 112, he gave a wide generalization of the number (B), which was only rediscovered, apparently, several years ago.

\(^7\) Nachr. Ges. Wiss. Göttingen, Math.-physik. Kl., 1–11, 427–455, 1927. A historical note appears in order here. I spent several months in Zurich in 1928 and visited with Professor Fueter a number of times. He talked to me a great deal about the contents of the above papers and how these ideas generalized a large part of the material given by Hilbert in his Jahresber. Deutsch. Math.-Vereinigung “Report on Algebraic Numbers” (Œuvres, 1, 195–248). There is a connection here with the remarks made by Hilbert at the end of the third chapter (p. 194), which treated the theory of quadratic fields, and at the end of this chapter he refers to a “Höheren Theorie” of quadratic fields obtained by adjoining other fields to the quadratic. He then says: “Die theorie der zu einem imaginären quadratischen Körper gehörigen Klassenkörper sowie der dazu gehörigen relativ-Abelschen Körper erfordert jedoch zu ihrem Aufbau die Methode der komplexen Multiplikation der elliptischen Funktionen, und dies ist ein Gegenstand, welcher von der Aufnahme in diesen Bericht ausgeschlossen werden müsste.”

Fueter told me that Hilbert had been to see him in Zurich and had remarked that the reason he had omitted the use of the complex multiplication of elliptic functions in the report was that...
this subject had not been sufficiently developed, as far as possible applications to number theory were concerned, at the time he wrote his report. Hilbert also said that he was very glad to hear that Fueter had fashioned the necessary tools from the theory of elliptic functions to yield an advanced theory of quadratic fields.

We hope to be able to discuss in a later paper the methods of Fueter in their relation to the class field theory as it has been developed up to the present. As to the work of Fueter's predecessors in this line, cf. H. Hasse, Jahresber. Deut. Math.-, Vereinigung, 35, 39–44, 1926.

---

ON CYCLOTOMIC RELATIONS AND TRINOMIAL EQUATIONS IN A FINITE FIELD

BY H. S. VANDIVER

DEPARTMENT OF MATHEMATICS AND ASTRONOMY, UNIVERSITY OF TEXAS

Communicated July 22, 1955

Let \( p \) be an odd prime and \( F[p^n] \) denote a finite field of order \( p^n \) and consider the solutions \( s, t \) of

\[
g^{i+cs} + g^{j+ct} = 1, \tag{1}
\]

where \( g \) is a multiplicative generator of the nonzero elements of \( F[p^n] \); \( i \) is a fixed integer in the set \( 0, 1, \ldots, c - 1 \); \( j \) is a fixed integer in the set \( 0, 1, \ldots, l - 1 \); \( p^n - 1 = cl \); \( s \) is in the range \( 0, 1, \ldots, l - 1 \); \( t \) is in the range \( 0, 1, \ldots, c - 1 \).

Let the number of sets of solutions \( s, t \) of the type above be \( (i, j)_{sl} \). Then (noting relation [2] of the present paper) the maximum value of the \( (i, j)_{sl} \) is \( l \) if \( c \geq l \). If there exists a \( j \) for a fixed \( i \) such that \( (i, j)_{sl} = l \), we shall call this “case A” of (1).

In several previous papers various consequences of this assumption were obtained, and the relation of some of them to Fermat’s Last Theorem was brought out. Other results of this type will be derived in the present paper.

To obtain the desired results concerning (1), it will be convenient to first write equation (1) in another form, and we shall also set \( l = m \), with \( m \) an odd prime, and assume that \( c \equiv 0 \pmod{l} \). Let \( [i, j] \) denote the number of solutions of the equation

\[
g^{i+cs'} + 1 = g^{j+t'}
\]

in a finite field \( F(p^n) \) of order \( p^n = lc + 1 \), \( s' \) being in the range \( 0, 1, \ldots, l - 1 \), and \( t' \) in the range \( 0, 1, \ldots, c - 1 \), for given \( i \) and \( j \). It is known that

\[
\sum_{i=0}^{l-1} [i, j] = l - \begin{cases} 
0 & \text{if } i \equiv c \pmod{2}, \\
1 & \text{if } i \equiv c \pmod{2}.
\end{cases}
\]

Evidently \([i, j] = [i + ca, j + 2\gamma]\). Let \( g \) be a primitive root in the finite field of order \( p^n \) and \( g^s = y \), with \( x \) an integer and \( y \) an element of the \( F(p^n) \). We write

\[
\text{ind } y \equiv x \pmod{p^n - 1}.
\]

It is known that